

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-335239

(43)Date of publication of application : 22.11.2002

(51)Int.Cl.

H04L 9/32

G06F 15/00

G09C 1/00

H04L 9/08

(21)Application number : 2001-138736

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 09.05.2001

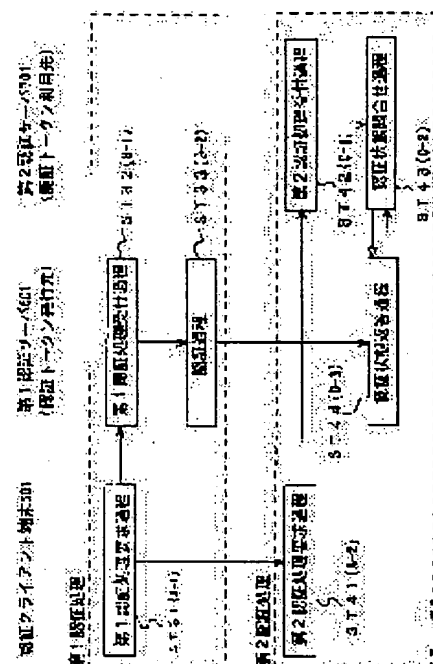
(72)Inventor : ITO KOJI
MORIMURA KAZUO

(54) METHOD AND SYSTEM DEVICE FOR AUTHENTICATING SINGLE SIGN- ON

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and system device for authenticating signal sign-on which enable reduction of a system construction cost and an operation managing cost by realizing a single sign-on function without requiring an authentication state managing server for unitarily managing an authentication state.

SOLUTION: This characteristic configuration method comprises first authentication processing where a first authentication server 601 to which a contents request (ST31) is applied from an authentication client terminal 501 operated by a user, performs (ST32) the authentication of the user, holds the authentication state as a result of the authentication performance and prepares/issues (ST33) an authentication token showing the authentication state and second authentication processing where a second authentication server 701 to which a contents request (ST41) is applied from the authentication client terminal 501 operated by the user and which accepts the request, performs processing (ST43) concerning the authentication of the user by utilizing (ST44) the authentication token prepared/issued in the first authenticating processing.



LEGAL STATUS

[Date of request for examination]

01.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection]

[Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-335239

(P2002-335239A)

(43) 公開日 平成14年11月22日 (2002. 11. 22)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
H 0 4 L 9/32		G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
G 0 6 F 15/00	3 3 0	G 0 9 C 1/00	6 4 0 D 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 D
H 0 4 L 9/08			6 0 1 C

審査請求 未請求 請求項の数15 O L (全 19 頁)

(21) 出願番号 特願2001-138736(P2001-138736)

(22) 出願日 平成13年5月9日(2001.5.9)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 伊藤 浩二

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者 森村 一雄

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100071113

弁理士 菅 隆彦

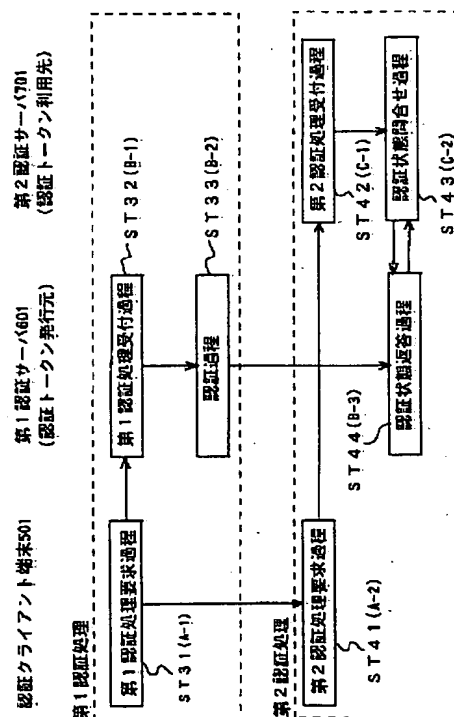
最終頁に続く

(54) 【発明の名称】 シングルサインオン認証方法及びシステム装置

(57) 【要約】

【課題】 認証状態を一元管理する認証状態管理サーバを必要とせずに、シングルサインオン機能を実現して、システム構築コスト及び運用管理コストを軽減することを可能とするシングルサインオン認証方法及びシステム装置の提供。

【解決手段】 ユーザが操作する認証クライアント端末501からコンテンツ要求(ST31)された第1認証サーバ601が、当該ユーザの認証を実行(ST32)して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成発行(ST33)する第1認証処理と、ユーザが操作する認証クライアント端末501からコンテンツ要求(ST41)され、受付た(ST42)第2認証サーバ701が、第1認証処理で作成発行された認証トークンを利用(ST44)して、当該ユーザの認証についての処理(ST43)を行なう第2認証処理と、を実施してなる特徴的構成手法の採用。



1

【特許請求の範囲】

【請求項 1】特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、前記複数のサーバにおける個々のサーバがユーザの認証状態を分散管理する、ことを特徴とするシングルサインオン認証方法。

【請求項 2】特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、ユーザが操作する認証クライアント端末からコンテンツの要求をされた第 1 認証サーバが、当該ユーザの認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成する第 1 認証処理と、ユーザが操作する認証クライアント端末からコンテンツの要求をされた第 2 認証サーバが、前記第 1 認証処理で作成された前記認証トークンを利用して、当該ユーザの認証についての処理を行なう第 2 認証処理と、を実施してなる、ことを特徴とするシングルサインオン認証方法。

【請求項 3】前記第 1 認証処理は、前記認証クライアント端末が前記第 1 認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第 1 認証処理要求過程と、当該第 1 認証処理要求過程で生じた認証処理の要求を前記第 1 認証サーバが受け付ける第 1 認証処理受付過程と、当該第 1 認証処理受付過程で受けつけられた認証処理の要求につき、認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成して、前記認証クライアント端末に発行する認証過程と、を順次一貫経由して実施してなり、前記第 2 認証処理は、前記認証クライアント端末が前記第 2 認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第 2 認証処理要求過程と、当該第 2 認証処理要求過程で生じた認証処理の要求を前記第 2 認証サーバが受け付ける第 2 認証処理受付過程と、当該第 2 認証処理受付過程で受けつけられた認証処理の要求につき、前記第 1 認証処理の認証過程で作成された前記認証トークンであって前記認証クライアント端末から送信された前記認証トークンに基づいて、前記第 2 認証サーバが、当該認証トークンの発行元である前記第 1

2

認証サーバに当該認証トークンの有効性を問合せる認証状態問合せ過程と、当該認証状態問合せ過程で生じた前記認証トークンの有効性の問合せに対して、前記第 1 認証サーバが前記認証クライアント端末についてのユーザの認証状態を前記第 2 認証サーバに送信する認証状態返答過程と、を順次一貫経由して実施してなる、ことを特徴とする請求項 2 に記載のシングルサインオン認証方法。

10 【請求項 4】前記認証過程は、前記認証トークンを発行するときに、当該認証トークンの発行元である前記第 1 認証サーバを特定するものとなる電子的な署名を、当該認証トークンに含ませる署名作成処理をも実施する、ことを特徴とする請求項 3 に記載のシングルサインオン認証方法。

【請求項 5】前記認証過程は、前記第 1 認証サーバ及び前記第 2 認証サーバで共有する共通鍵を用いて、前記認証トークンを暗号化して、前記 20 認証クライアント端末に発行する共通鍵暗号処理をも実施する、ことを特徴とする請求項 4 に記載のシングルサインオン認証方法。

【請求項 6】前記シングルサインオン認証方法は、前記第 1 認証サーバ及び前記第 2 認証サーバのそれぞれが、認証に関する各サーバの信頼性を表すパラメータとなる認証レベルを保持しており、前記第 2 認証処理は、前記認証トークンを受け取ったときに、当該第 1 認証サーバの認証レベルと当該第 2 認証サーバの認証レベルとを比較して、当該比較の結果に基づいて前記認証状態を管理する認証トークン検査更新処理をも実施する、ことを特徴とする請求項 5 に記載のシングルサインオン 30 認証方法。

【請求項 7】前記認証トークン検査更新処理は、前記第 1 認証サーバの認証レベルよりも前記第 2 認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第 2 認証サーバで管理すると共に、当該第 1 認証サーバで管理されていた前記認証状態を破棄させ、40 前記第 2 認証サーバの認証レベルよりも前記第 1 認証サーバの認証レベルの方が高い場合は、前記認証状態をそのまま当該第 1 認証サーバで管理させる、処理からなる、ことを特徴とする請求項 6 に記載のシングルサインオン認証方法。

【請求項 8】前記認証トークン検査更新処理は、前記認証トークンを前記共通鍵を用いて復号化する共通鍵復号処理と、前記署名作成処理で前記認証トークンに含まれた署名を検証する署名検証処理と、50

3

前記認証トークンに含まれるユーザの認証IDを検証する認証ID検証処理と、

前記認証トークンに含まれる情報であって前記認証クライアント端末を特定する情報を検証するクライアント情報検証処理と、

前記認証トークンに含まれる情報である当該認証トークンの有効期限を検証する有効期限検証処理と、を実施して、

前記認証トークンの有効性を判断する処理も併せ実施する、

ことを特徴とする請求項7に記載のシングルサインオン認証方法。

【請求項9】特定のユーザに限定したサービスの提供するために認証をするものにして、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証システム装置であって、

コンテンツを要求する認証クライアント端末と、

当該認証クライアント端末からのコンテンツ要求に応じて認証を実行し、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを当該認証クライアント端末に発行する第1認証サーバと、

前記認証クライアント端末からのコンテンツ要求に応じて認証を実行するときに、当該認証クライアント端末から前記認証トークンを受け取り、当該認証トークンの発行元である前記第1認証サーバに当該認証トークンの有効性につき問合せる第2認証サーバと、を有する、

ことを特徴とするシングルサインオン認証システム装置。

【請求項10】前記第1認証サーバは、前記認証トークンを発行するときに、当該認証トークンの発行元である当該第1認証サーバを特定するものとなる電子的な署名を、当該認証トークンに付する署名作成部を有する、

ことを特徴とする請求項9に記載のシングルサインオン認証システム装置。

【請求項11】前記第1認証サーバは、当該第1認証サーバ及び前記第2認証サーバで共有する共通鍵を用いて、前記認証トークンを暗号化する共通鍵暗号部を有し、

当該共通鍵暗号部で暗号化された前記認証トークンを前記認証クライアント端末に発行自在な構成とする、

ことを特徴とする請求項10に記載のシングルサインオン認証システム装置。

【請求項12】前記第2認証サーバは、前記認証トークンを受け取ったときに、前記第1認証サーバの認証レベルと当該第2認証サーバの認証レベルとを比較して、

当該第1認証サーバの認証レベルよりも当該第2認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第2認証サーバで管理すると共に、当該第1認証サーバ

4

バで管理されていた前記認証状態を破棄自在な構成とする、

ことを特徴とする請求項9、10又は11に記載のシングルサインオン認証システム装置。

【請求項13】前記第1認証サーバ及び前記第2認証サーバは、

それぞれ、前記認証トークンの発行先を限定する信頼されるサーバリストを有し、

当該信頼されるサーバリストに挙げられているサーバに対してのみ、前記認証トークンを発行自在な構成とする、

ことを特徴とする請求項12に記載のシングルサインオン認証システム装置。

【請求項14】前記第1認証サーバ及び前記第2認証サーバは、

それぞれ、受け取った前記認証トークンの信頼判断に用いる信頼するサーバリストを有し、

受け取った前記認証トークンが当該信頼するサーバリストに挙げられているサーバが発行したものであるか確認自在な構成とする、

ことを特徴とする請求項13に記載のシングルサインオン認証システム装置。

【請求項15】前記第1認証サーバ及び前記第2認証サーバは、

それぞれ、

認証対象のユーザのIDと、当該ユーザのパスワードと、当該ユーザを特定する情報とを、相互に関連付けて保持する認証データベースと、

認証済みのユーザのIDと、当該ユーザのアクセスごとに変更される一時的なIDと、当該ユーザに操作される前記認証クライアント端末のアドレスと、当該ユーザの認証状態の有効期限と、当該ユーザを特定する情報とを、相互に関連付けて保持する認証状態管理データベースと、

を有してなる、

ことを特徴とする請求項14に記載のシングルサインオン認証システム装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネットを始めとするネットワーク上に存在する複数のサーバ（サーバ）において、ユーザの認証状態を共有し、特定のユーザに限定してサービスを提供するシステムに好適なものに関し、特に、認証状態を集中して管理するサーバを必要とせずに、複数の認証サーバで作成された認証状態を分散管理して相互に共通利用することを可能とするシングルサインオン認証方法及びシステム装置に関するものである。

【0002】即ち、本発明は、ネットワーク上に存在する複数のサーバが認証状態を共用するシステムに好適な

シングルサインオン認証方法及びシステム装置に関するものである。ここで、認証状態とは、ユーザが既に認証済みであるか否かについての状態をいう。

【0003】

【従来の技術】従来、ユーザが1回のログインで、複数のサーバにアクセスできるようにするシングルサインオン(single signon)という機能が考え出されている。複数のサーバが個々に認証を行なうと、ユーザはさまざまなユーザIDとパスワードを使い分ける必要が生じる。

【0004】また管理という観点からも、複数パスワードを定期的に更新する手間を考えると、好ましくない。こうした環境において、ユーザの利便性と管理機能を向上させるため、ディレクトリサービスと同期して、複数サーバの認証とユーザのアクセス制御を一元管理するのがシングルサインオンとよばれる機能である。

【0005】また、従来、ネットワーク上に存在する複数のサーバにおいて、シングルサインオンを用いて認証状態を共有し、特定のユーザに限定したサービスを提供するためには、認証状態を集中管理する認証状態管理サーバを設けていた。そして、各認証サーバが、ユーザの認証をする際に、認証状態管理サーバにユーザの認証状態を問合せることで、複数のサーバ間で認証状態を共有していた。

【0006】図12は、従来のシングルサインオン機能を持ったシステム装置の模式概念図である。同図において、認証クライアント端末101は、パーソナルコンピュータ、PDA(Personal Digital Assistants)などからなる端末であり、処理プログラム102を内蔵している。

【0007】インターネット又はイントラネット上には、認証クライアント端末101の他に、複数の認証サーバ201、301が存在し、その認証サーバ201、301はそれぞれ処理プログラム202、302を内蔵している。また、認証サーバ201、301は、それぞれ、認証処理が終了した後にクライアントに提供するコンテンツ203、303を持っている。

【0008】更に、インターネット又はイントラネット上には、各認証サーバ201、301からの要求に応じて実際に認証処理及び認証状態の保持をする認証状態管理サーバ401が存在する。認証状態管理サーバ401は、処理プログラム402と、ID又はパスワードなどのユーザを認証するための情報を格納する認証データベース403と、ユーザの認証状態を保持する認証状態管理データベース404を持っている。

【0009】図13は、図12に示す従来のシステム装置の処理手順を示すフローチャートである。ここでは、ユーザが認証クライアント端末101によって認証サーバ201(認証状態発行元)にアクセスして認証手続きを行なった後、認証サーバ301(認証状態利用先)に

アクセスする場合を仮定する。

【0010】先ず、認証処理要求過程ST11(A-1)からの認証要求は、認証処理受付過程ST12(B-1)で受け付けられた後、認証過程ST13(D-1)において認証処理及び認証状態の格納が行われる。その後、再び他の認証サーバ301に対して認証処理要求過程ST21(A-2)からの認証要求が発生した場合は、認証処理受付過程ST22(C-1)で受け付けられた後、認証過程ST23(D-2)において認証処理及び認証状態の格納が行われる。

【0011】このとき、認証過程ST13(D-1)で作成した認証状態が既に存在する場合は、その認証状態の情報を利用して認証が行われ、ユーザが認証に関する処理を再び行う必要はない。これらのように、複数の認証サーバ201、301が認証を行う場合に、認証状態の管理を認証状態管理サーバ401が一括して行うことにより、認証状態を共有してシングルサインオンを実現している。

【0012】

【発明が解決しようとする課題】上述のように、従来は、ネットワーク上に存在する複数のサーバ(認証サーバ201、301)において、認証状態を共有し、特定のユーザに限定したサービスを提供するために、認証状態を特設した専門の認証状態管理サーバ401において一元的に管理している。これにより、認証状態を確実に管理し、ユーザが認証に関わる作業を繰り返し行う必要がなくなるシングルサインオンが実現する。

【0013】しかしながら、このような従来の手法では、認証状態管理サーバ401に処理が集中するため、認証状態管理サーバ401には特に高い処理能力が求められ、多額の運用資金と高度な運用スキルが求められる。このことにより小規模サイトにおいては、シングルサインオンとして運用することがコスト面及び運用面で困難なものとなっている。

【0014】また、従来の手法では、ネットワーク上においてシングルサインオンを実現するときに、シングルサインオンを実施するサーバ群の認証状態の信頼性は常に均一となっているものではなく、各サーバ間で信頼性の高低が生ずる。また、ネットワーク上で認証状態を交換するときに、盗聴、改ざん、成りすまし等のネットワーク特有の危険性も存在している。

【0015】ここにおいて、本発明の解決すべき主要な目的は以下の通りである。即ち、本発明の第1の目的は、ユーザが1回のログインで複数のサーバにアクセス可能となるシングルサインオン機能を持つシステムについて、認証状態を一元管理する認証状態管理サーバを必要とせずに、システム構築コスト及び運用管理コストを軽減することを可能とするシングルサインオン認証方法及びシステム装置を提供せんとするものである。

【0016】本発明の第2の目的は、複数の認証サーバ

間において認証に関する信頼性につき優劣があっても、認証状態の適切な管理を可能とするシングルサインオン認証方法及びシステム装置を提供せんとするものである。

【0017】本発明の第3の目的は、複数の認証サーバ（サーバ）間でネットワークを介して認証状態を相互に利用しても、セキュリティを確保することを可能とするシングルサインオン認証方法及びシステム装置を提供せんとするものである。

【0018】本発明の他の目的は、明細書、図面、特に、特許請求の範囲における各請求項の記載から自ずと明らかとなる。

【0019】

【課題を解決するための手段】本発明装置は、上記課題の解決に当たり、ユーザが既に認証済みであるかの状態を示す認証状態を、選択分散管理する複数の認証サーバを有してなる構成手段を講じる特徴を有する。

【0020】本発明方法は、上記課題の解決に当たり、認証サーバは、他の認証サーバによって認証された情報である認証トークンを認証クライアント端末から受け取った際に、認証トークン発行元の認証サーバに対する問合せ電文を作成して、受け取った認証トークンの有効性を検証する構成手法を講じる特徴を有する。

【0021】更に、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法又は手段を採用することにより、上記目的を達成するように為される。

【0022】即ち、本発明方法の第1の特徴は、特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、前記複数のサーバにおける個々のサーバがユーザの認証状態を分散管理してなるシングルサインオン認証方法の構成採用にある。

【0023】本発明方法の第2の特徴は、特定のユーザに限定したサービスの提供をするために認証をするシステムに供され、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証方法であって、ユーザが操作する認証クライアント端末からコンテンツの要求をされた第1認証サーバが、当該ユーザの認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成する第1認証処理と、ユーザが操作する認証クライアント端末からコンテンツの要求をされた第2認証サーバが、前記第1認証処理で作成された前記認証トークンを利用して、当該ユーザの認証についての処理を行なう第2認証処理と、を実施してなるシングルサインオン認証方法の構成採用にある。

【0024】本発明方法の第3の特徴は、上記本発明方法の第2の特徴における前記第1認証処理が、前記認証

クライアント端末が前記第1認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第1認証処理要求過程と、当該第1認証処理要求過程で生じた認証処理の要求を前記第1認証サーバが受け付ける第1認証処理受付過程と、当該第1認証処理受付過程で受け付けられた認証処理の要求につき、認証を実行して、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを作成して、前記認証クライアント端末に発行する認証過程と、を順次一貫経由して実施してなり、前記第2認証処理は、前記認証クライアント端末が前記第2認証サーバに対してコンテンツを要求することに応じて、当該認証クライアント端末についてのユーザの認証処理を要求する第2認証処理要求過程と、当該第2認証処理要求過程で生じた認証処理の要求を前記第2認証サーバが受け付ける第2認証処理受付過程と、当該第2認証処理受付過程で受け付けられた認証処理の要求につき、前記第1認証処理の認証過程で作成された前記認証トークンであって前記認証クライアント端末から送信された前記認証トークンに基づいて、前記第2認証サーバが、当該認証トークンの発行元である前記第1認証サーバに当該認証トークンの有効性を問合せる認証状態問合せ過程と、当該認証状態問合せ過程で生じた前記認証トークンの有効性の問合せに対して、前記第1認証サーバが前記認証クライアント端末についてのユーザの認証状態を前記第2認証サーバに送信する認証状態返答過程と、を順次一貫経由して実施してなるシングルサインオン認証方法の構成採用にある。

【0025】本発明方法の第4の特徴は、上記本発明方法の第3の特徴における前記認証過程が、前記認証トークンを発行するときに、当該認証トークンの発行元である前記第1認証サーバを特定するものとなる電子的な署名を、当該認証トークンに含ませる署名作成処理をも実施してなるシングルサインオン認証方法の構成採用にある。

【0026】本発明方法の第5の特徴は、上記本発明方法の第4の特徴における前記認証過程が、前記第1認証サーバ及び前記第2認証サーバで共有する共通鍵を用いて、前記認証トークンを暗号化して、前記認証クライアント端末に発行する共通鍵暗号処理をも実施してなるシングルサインオン認証方法の構成採用にある。

【0027】本発明方法の第6の特徴は、上記本発明方法の第5の特徴における前記シングルサインオン認証方法が、前記第1認証サーバ及び前記第2認証サーバのそれぞれが、認証に関する各サーバの信頼性を表すパラメータとなる認証レベルを保持しており、前記第2認証処理は、前記認証トークンを受け取ったときに、当該第1認証サーバの認証レベルと当該第2認証サーバの認証レベルとを比較して、当該比較の結果に基づいて前記認証状態を管理する認証トークン検査更新処理をも実施して

10

20

30

40

50

なるシングルサインオン認証方法の構成採用にある。

【0028】本発明方法の第7の特徴は、上記本発明方法の第6の特徴における前記認証トークン検査更新処理が、前記第1認証サーバの認証レベルよりも前記第2認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第2認証サーバで管理すると共に、当該第1認証サーバで管理されていた前記認証状態を破棄させ、前記第2認証サーバの認証レベルよりも前記第1認証サーバの認証レベルの方が高い場合は、前記認証状態をそのまま当該第1認証サーバで管理させる、処理からなるシングルサインオン認証方法の構成採用にある。

【0029】本発明方法の第8の特徴は、上記本発明方法の第7の特徴における前記認証トークン検査更新処理が、前記認証トークンを前記共通鍵を用いて復号化する共通鍵復号処理と、前記署名作成処理で前記認証トークンに含められた署名を検証する署名検証処理と、前記認証トークンに含まれるユーザの認証IDを検証する認証ID検証処理と、前記認証トークンに含まれる情報であって前記認証クライアント端末を特定する情報を検証するクライアント情報検証処理と、前記認証トークンに含まれる情報である当該認証トークンの有効期限を検証する有効期限検証処理と、を実施して、前記認証トークンの有効性を判断する処理も併せ実施してなるシングルサインオン認証方法の構成採用にある。

【0030】本発明装置の第1の特徴は、特定のユーザに限定したサービスの提供をするために認証をするものにして、ネットワーク上に存在する複数のサーバがユーザの認証状態を共有するシングルサインオン認証システム装置であって、コンテンツを要求する認証クライアント端末と、当該認証クライアント端末からのコンテンツ要求に応じて認証を実行し、当該認証実行の結果である認証状態を保持し、当該認証状態を示す認証トークンを当該認証クライアント端末に発行する第1認証サーバと、前記認証クライアント端末からのコンテンツ要求に応じて認証を実行するときに、当該認証クライアント端末から前記認証トークンを受け取り、当該認証トークンの発行元である前記第1認証サーバに当該認証トークンの有効性につき問合せする第2認証サーバと、を有してなるシングルサインオン認証システム装置の構成採用にある。

【0031】本発明装置の第2の特徴は、上記本発明装置の第1の特徴における前記第1認証サーバが、前記認証トークンを発行するときに、当該認証トークンの発行元である当該第1認証サーバを特定するものとなる電子的な署名を、当該認証トークンに付する署名作成部を有してなるシングルサインオン認証システム装置の構成採用にある。

【0032】本発明装置の第3の特徴は、上記本発明装置の第2の特徴における前記第1認証サーバが、当該第1認証サーバ及び前記第2認証サーバで共有する共通鍵

を用いて、前記認証トークンを暗号化する共通鍵暗号部を有し、当該共通鍵暗号部で暗号化された前記認証トークンを前記認証クライアント端末に発行自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【0033】本発明装置の第4の特徴は、上記本発明装置の第1、第2又は第3の特徴における前記第2認証サーバが、前記認証トークンを受け取ったときに、前記第1認証サーバの認証レベルと当該第2認証サーバの認証レベルとを比較して、当該第1認証サーバの認証レベルよりも当該第2認証サーバの認証レベルの方が高い場合は、前記認証状態を当該第2認証サーバで管理すると共に、当該第1認証サーバで管理されていた前記認証状態を破棄自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【0034】本発明装置の第5の特徴は、上記本発明装置の第4の特徴における前記第1認証サーバ及び前記第2認証サーバが、それぞれ、前記認証トークンの発行先を限定する信頼されるサーバリストを有し、当該信頼されるサーバリストに挙げられているサーバに対してのみ、前記認証トークンを発行自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【0035】本発明装置の第6の特徴は、上記本発明装置の第5の特徴における前記第1認証サーバ及び前記第2認証サーバが、それぞれ、受け取った前記認証トークンの信頼判断に用いる信頼するサーバリストを有し、受け取った前記認証トークンが当該信頼するサーバリストに挙げられているサーバが発行したものであるか確認自在な構成としてなるシングルサインオン認証システム装置の構成採用にある。

【0036】本発明装置の第7の特徴は、上記本発明装置の第6の特徴における前記第1認証サーバ及び前記第2認証サーバが、それぞれ、認証対象のユーザのIDと、当該ユーザのパスワードと、当該ユーザを特定する情報とを、相互に関連付けて保持する認証データベースと、認証済みのユーザのIDと、当該ユーザのアクセスごとに変更される一時的なIDと、当該ユーザに操作される前記認証クライアント端末のアドレスと、当該ユーザの認証状態の有効期限と、当該ユーザを特定する情報とを、相互に関連付けて保持する認証状態管理データベースと、を有してなるシングルサインオン認証システム装置の構成採用にある。

【0037】これらにより、本発明は、従来認証状態管理サーバが一元管理していた認証状態を、個々の認証サーバが相互に認証レベルを比較して選択分散管理するので、従来必要とされた認証状態管理サーバの運用・構築コストを削減することができる。即ち、個々の認証サーバは、他の認証サーバによって認証された情報（認証トークン）を認証クライアント端末から受け取った際に、認証トークン発行元の認証サーバに対する問合せ電文を

作成し、受け取った認証トークンの有効性を検証する。

【0038】また、本発明の選択分散管理は、複数の認証サーバ間における認証に関する信頼性の優劣を意識した認証状態の適切な管理を行うために、それぞれの認証サーバ（サーバ）に認証に関する信頼性を表すパラメータ（認証レベル）を付与する。そして、認証トークン発行元の認証サーバに認証トークンの有効性を確認する際に、認証トークン発行元の認証サーバの認証レベルが認証トークン利用先の認証サーバの認証レベルを上回る場合は、認証状態はそのまま認証トークン発行元の認証サーバで管理される。

【0039】一方、認証トークン発行元の認証サーバの認証レベルが認証トークン利用先の認証レベルを下回る場合は、認証状態は新たに認証トークン利用先において管理されると共に、認証トークン発行元の認証サーバで管理されていた情報（認証状態）は破棄される。このような手段を用いることにより、本発明によれば、各認証サーバ（サーバ）間に認証レベルの優劣が存在する場合における認証状態の適切な管理が可能となる。

【0040】更に、本発明は、各認証サーバ（サーバ）間の認証状態の相互利用におけるセキュリティ維持について、各認証サーバは相互に共通な共通鍵を持ち、問合せ電文及び応答電文の暗号化を行う。また、各認証サーバは、それぞれ「信頼するサーバの一覧」と「信頼されるサーバの一覧」を持ち、認証トークン発行時には信頼されるサーバに対して認証トークンを発行し、他のサーバが発行した認証トークンを利用する場合には信頼するサーバが発行した認証トークンであることを確認する。

【0041】更にまた、本発明は、認証サーバ間でやり取りされる電文は各認証サーバの秘密鍵により電子的に署名され、認証状態の偽造・改ざん・なりすましを防止する。これらにより、本発明は、認証状態を選択分散管理して、安全、簡易且つ柔軟に認証状態を共有することを可能とする。

【0042】

【発明の実施の形態】以下、添付図面を参照しながら、本発明の実施の形態を装置例及び方法例につき説明する。

【0043】なお、本発明は、ネットワーク上において、ユーザの認証状態を複数のサーバが共有して、ユーザが1回のログインで複数のサーバにアクセスできるようにするシングルサインオンをなすものであって、認証状態を複数のサーバで選択分散管理するものであるが、本実施形態では、ネットワークとしてとして専らインターネット/イントラネットを代表例として説明するも、本発明はこれ等に限定されるものではない。

【0044】（装置例）図1は、本発明の装置例に係るシングルサインオン認証システム装置の概念模式図である。図中、2はインターネット及びイントラネットなどからなるネットワーク、501はパーソナルコンピュー

タ又はPDAなどからなる認証クライアント端末である。

【0045】601は認証クライアント端末からのコンテンツ要求に応じて認証を実行する第1認証サーバ、701は認証クライアント端末からのコンテンツ要求に応じて認証を実行する第2認証サーバである。認証クライアント端末501、第1認証サーバ601及び第2認証サーバ701は、相互にネットワーク2を介して接続される。

【0046】認証クライアント端末501は、第1認証サーバ601及び第2認証サーバ701に対してコンテンツを要求するものであり、自身の動作を規定する処理プログラム502を内蔵している。第1認証サーバ601は、自身の動作を規定する処理プログラム602を内蔵している。第2認証サーバ701は、自身の動作を規定する処理プログラム702を内蔵している。

【0047】また、第1認証サーバ601は、認証したクライアント（認証クライアント端末501）に対して送信するWWWコンテンツ603と、認証処理に用いるデータからなる認証データベース604と、認証状態の保持及び管理をする認証状態管理データベース605と、認証トークンの発行先を限定する「信頼されるサーバリスト」606と、受け取った認証トークンを信頼するか否かの判断に用いる信頼するサーバリスト607とを備えている。

【0048】第2認証サーバ701も、第1認証サーバ601と同様に、認証したクライアント（認証クライアント端末501）に対して送信するWWWコンテンツ703と、認証処理に用いるデータからなる認証データベース704と、認証状態の保持及び管理をする認証状態管理データベース705と、認証トークンの発行先を限定する「信頼されるサーバリスト」706と、受け取った認証トークンを信頼するか否かの判断に用いる「信頼するサーバリスト」707とを備えている。

【0049】ここで、認証トークンとは、各クライアントの認証状態を示す情報からなるものであり、認証クライアント端末501からのコンテンツ要求に応じて、第1認証サーバ601（又は第2認証サーバ701）が認証する際に作成されるものであり、詳細は後述する。

【0050】本実施形態では、第1認証サーバ601を認証トークン発行元として、第2認証サーバ701を認証トークン利用先としているが、これは説明上仮定したものである。即ち、第1認証サーバ601と第2認証サーバ701は、それぞれ同じ機能を持ち、それぞれ認証トークン発行元になり且つ認証トークン利用先ともなる。

【0051】即ち、第1認証サーバ601は、認証クライアント端末501からのコンテンツ要求に応じて認証を実行し、当該認証実行の結果である認証状態を認証状態管理データベース605で保持及び管理し、当該認証

10

20

30

40

50

状態を示す認証トークンを当該認証クライアント端末に発行するものである。

【0052】第2認証サーバ701は、認証クライアント端末501からのコンテンツ要求に応じて認証を実行するときに、認証クライアント端末501から認証トークンを受け取り、その認証トークンの発行元である第1認証サーバ601に当該認証トークンの有効性につき問合せるものである。

【0053】図2は、本装置例に係るシングルサインオン認証システム装置の動作を示すフローチャートである。本図では、第1認証処理として、ユーザが認証クライアント端末501から第1認証サーバ601（認証トークン発行元）にアクセスして認証手続きを行った後、第2認証処理として、第2認証サーバ701（認証トークン利用先）にアクセスする場合を仮定して、示している。

【0054】まず、認証クライアント端末501で実行される認証処理要求過程ST31（A-1）からの認証要求は、第1認証サーバ601の認証処理受付過程ST32（B-1）で受け付けられた後、第1認証サーバ601の認証過程ST33（B-2）で認証処理及び認証状態の格納が行われる。

【0055】その後、再び認証クライアント端末501において、認証処理要求過程ST41（A-2）からの認証要求が他のサーバ（第2認証サーバ701）に対して発生した場合は、その認証要求が第2認証サーバ701の認証処理受付過程ST42（C-1）で受け付けられる。

【0056】ここで、他のサーバ（第1認証サーバ601）によって認証された認証トークンがその認証要求に添付されている場合には、第2認証サーバ701の認証状態問合せ過程ST43（C-2）で、第1認証サーバ601の認証状態返答過程ST44（B-3）に対しての認証状態についての問合せが実行される。

【0057】そして、第2認証サーバ701の認証状態問合せ過程ST43（C-2）において、認証トークンの有効性につき確認され、有効性が確認された場合はいずれのサーバ（第1認証サーバ601又は第2認証サーバ701）が認証状態を保持及び管理すべきかの判定が行われ、その判定に基づいて認証状態の保持及び管理が実行される。

【0058】これらにより、第1認証処理における認証過程ST33（B-1）で認証状態が作成されるので、第2認証処理においては認証過程ST33（B-1）で作成された認証状態を利用して認証が行われ、ユーザが認証に関する処理を再び行う必要はない。

【0059】図3は、第1認証サーバ601及び第2認証サーバ701がそれぞれ具備するデータベースの構造を示す図である。

【0060】図中、（a）は認証データベース604、

704の構造を示し、（b）は認証状態管理データベース605、705の構造を示している。認証データベース604、704は、認証対象のユーザのIDであるユーザIDと、当該ユーザのパスワードと、当該ユーザを特定する情報などを、相互に関連付けて保持するものである。

【0061】認証状態管理データベース605、705は、認証済みのユーザのIDであるユーザIDと、当該ユーザのアクセスごとに変更される一時的なIDである認証IDと、当該ユーザに操作される認証クライアント端末501のアドレスと、当該ユーザの認証状態の有効期限と、当該ユーザを特定する情報とを、相互に関連付けて保持するものである。

【0062】次に、本実施形態の方法例として、あるユーザが第1認証サーバ601において認証をした後、

1）再び、同じサーバである第1認証サーバ601に対して認証をする場合、

2）異なるサーバである第2認証サーバ701に対して認証を行う場合であって、（第1認証サーバ601の認証レベル） \geq （第2認証サーバ701の認証レベル）である場合、

3）異なるサーバである第2認証サーバ701に対して認証を行う場合であって、（第1認証サーバ601の認証レベル） $<$ （第2認証サーバ701の認証レベル）である場合、

の3通りの場合に分けて、説明する。

【0063】ここで、認証レベルとは、各認証サーバに付されるものであって、認証に関する各認証サーバの信頼性を表すパラメータとなるものであり、認証レベルの高い認証サーバが管理する認証状態ほど、信頼性の高い認証がなされているものとする。

【0064】そして、各認証サーバ（第1認証サーバ601及び第2認証サーバ701）は、認証トークンを利用して認証状態を共有するので、第2認証サーバ701に対する認証時には、ユーザは認証処理を改めて行う必要がない。即ち、シングルサインオンが実行される。

【0065】（方法例1）前記装置例に適用する本実施形態例の方法例1につき図4乃至及び図8を参照して説明する。方法例1は、あるユーザが第1認証サーバ601において認証をした後、再び、同じサーバである第1認証サーバ601に対して認証をする場合に、適用される手法である。

【0066】図4は、ユーザが認証サーバ群に初めて認証を求めるときの手順を示すフローチャートである。いま、ユーザが認証サーバ群（第1認証サーバ601及び第2認証サーバ701）に対して、初めて認証をすると仮定する。即ち、認証クライアント端末501が第1認証サーバ601又は第2認証サーバ701に対して、初めてコンテンツの要求をする場合である。このときの処理手順が図3に示されている。

【0067】 先ず、ユーザは、認証クライアント端末501の処理プログラム502を起動させて、その処理プログラム502に含まれているコンテンツ要求部503から第1認証サーバ601の処理プログラム602の認証開始部608に対して、コンテンツを要求する。

【0068】 認証開始部608は、コンテンツの要求を受けた後、その要求内容が認証を必要とするものか判断し、認証が必要である場合は認証処理部609を呼び出す。認証処理部609は、コンテンツの要求に「認証済みの認証トークン」が付属していないことを確認し、認証データベース604から認証に必要なデータを取得して、認証処理を行う。

【0069】 ここで、認証が正常に完了した場合は、認証処理部609はコンテンツ返却部610を呼び出す。コンテンツ返却部610では、WWWコンテンツ603から要求に係るコンテンツを取得し、「信頼されるサーバリスト」606から認証トークンの配布先を取得し、認証トークン作成部611で作成された認証トークンを取得したコンテンツに添付して、そのコンテンツを認証クライアント端末501に返却する。

【0070】 図5は、認証トークン作成部611における処理手順を示すフローチャートである。図6は、第1認証サーバ601及び第2認証サーバ701で作成される各種電文の構造を示す概念模式図である。ここで、図6(a)は、認証トークン作成部611で作成された認証トークンの構造を示す概念模式図である。なお、図6(b)、(c)、(d)については後述する。

【0071】 先ず、認証トークン作成部611は、有効期限作成部612において指定された有効期限を作成する(有効期限作成処理)。その後、認証ID作成部613において乱数からなる認証IDを作成する(認証ID作成処理)。その後、作成された有効期限、認証ID及び認証クライアント端末501を特定するクライアント情報を認証状態管理データベース605に登録する。

【0072】 その後、署名作成部614において認証トークンを作成した認証サーバ(第1認証サーバ601)の署名を作成する(署名作成処理)。その後、共通鍵暗号部615において、認証トークン全体を各認証サーバが共通に持つ共通鍵によって暗号化する(共通鍵暗号処理)。そして、暗号化された認証トークンは、コンテンツ返却部610に送られ、コンテンツと共に認証クライアント端末501に送信される。

【0073】 次に、ユーザが過去に認証を求めた第1認証サーバに対して、再び認証を求める場合について説明する。図7は、同一の認証サーバに再度の認証要求が発生した場合の処理手順を示すフローチャートである。

【0074】 先ず、認証クライアント端末501の処理プログラム502が起動され、その処理プログラム502に含まれるコンテンツ要求部503から第1認証サーバ601の処理プログラム602の認証開始部608に

対して、コンテンツを要求する。

【0075】 その要求を受け取った認証開始部608は、その要求内容につき認証が必要か判断し、必要と判断した場合は認証処理部609を呼び出す。認証処理部609は、認証済みの認証トークンが、受け取ったコンテンツ要求に付属されていることを確認し、認証トークン検証/更新部616をよぶ。

【0076】 図8は、認証トークン検証/更新部616の処理手順を示すフローチャートである。認証トークン検証/更新部616では、先ず、認証トークン発行者検証部617が「信頼するサーバリスト607」を利用して、認証トークンの認証レベルを検証する。この方法例1では同一のサーバ(第1認証サーバ)が発行した認証トークンを同一のサーバ(第1認証サーバ)で利用するため、認証レベルの比較は不要となる。

【0077】 次に、共通鍵復号部618において認証トークンが共通鍵で復号化される(共通鍵復号処理)。引続き、署名検証部619において認証トークンに含まれる署名が検証される(署名検証処理)。その後、認証ID検証部620において前記認証トークンに含まれるユーザの認証IDが検証される(認証ID検証処理)。

【0078】 そして、クライアント情報検証部621において、認証トークンに含まれる情報であって認証クライアント端末501を特定する情報が検証される(クライアント情報検証処理)。更に、有効期限検証部622において認証トークンに含まれる情報である当該認証トークンの有効期限が検証される(有効期限検証処理)。

【0079】 これらに処理により、信頼できるサーバから有効な認証トークンが得られたことが検証される。その後、有効期限更新部623において新たな有効期限が作成され、認証ID更新部624において新たな認証IDが生成され、認証状態管理データベース605にその新たな有効期限及び認証IDが登録される。その後、署名作成部625においてクライアント情報と共に署名が生成され、共通鍵暗号部626において新たな認証トークンの全体が共通鍵で暗号化される。

【0080】 これらの処理の後、「信頼されるホストリスト606」を用いて認証トークンの配布先を特定し、コンテンツ返却部610は、WWWコンテンツ603から要求対象のコンテンツを取得して、新たな認証トークンと共に認証クライアント端末501に送付する。

【0081】 (方法例2) 前記装置例に適用する本実施形態例の方法例2につき図6及び図9を参照して説明する。方法例2は、あるユーザが第1認証サーバ601において認証をした後、第1認証サーバ601とは異なるサーバである第2認証サーバ701に対して認証をする場合に、適用される手法である。

【0082】 そして、方法例2では、第1認証サーバ601(認証トークン発行元)の認証レベルが、第2認証サーバ701(認証トークン利用先)の認証レベル以上

であると、仮定する。先ず、前述の方法例1と同様に、ユーザが認証サーバ群（第1認証サーバ601及び第2認証サーバ701）に対して、初めて認証を行うとする。その後、第1認証サーバ601とは異なる第2認証サーバ701に対して、認証要求を行うとする。このときの処理手順が図9に示されている。

【0083】図9は、認証トークン発行先の認証サーバの認証レベルが認証トークン利用先の認証サーバの認証レベル以上である場合の処理手順を示すフローチャートである。

【0084】先ず、ユーザは、認証クライアント端末501の処理プログラム502を起動させて、その処理プログラム502に含まれているコンテンツ要求部503から第2認証サーバ701の処理プログラム702の認証開始部708に対して、第1認証サーバ601で作成された認証トークンを伴ったコンテンツ要求情報を送信することで、コンテンツを要求する。

【0085】認証開始部708は、コンテンツ要求情報を受けた後、その要求内容が認証を必要とするものか判断し、認証が必要である場合は認証処理部709を呼び出す。認証処理部709は、コンテンツ要求情報に「認証済みの認証トークン」が付属していることを確認し、「信頼するサーバリスト707」を参照して、信頼するサーバによって作成された認証トークンであることを確認する。

【0086】その後、問合せ電文作成部727は、図6(b)に示す問合せ電文を作成し、認証トークン発行元の第1認証サーバ601の処理プログラム602の問合せ電文受付部629に暗号化された電文を送信する。

【0087】図6(b)は、問合せ電文作成部727で作成された問合せ電文の構造を示す概念模式図である。問合せ電文受付部629は、第1認証サーバ601と第2認証サーバ701の認証レベルを比較する。

【0088】その結果、第1認証サーバ601の認証レベルが第2認証サーバ701の認証レベル以上であると判断した場合は、認証トークン検査/更新部616において認証トークンを更新し、回答電文作成部630において図6(c)に示す回答電文を作成し、第2認証サーバ701の回答電文受付部728に送信する。

【0089】図6(c)は、回答電文作成部630で作成された回答電文の構造を示す概念模式図である。その後、回答電文受付部728は、受け取った新たな認証トークンと、その回答電文に含まれる「信頼されるサーバリスト」とをコンテンツ返却部710に渡す。

【0090】コンテンツ返却部710は、第1認証サーバ601から受け取った「信頼されるサーバリスト」に基づき、第1認証サーバ601から受け取った認証トークンを添付して、WWWコンテンツ703から取得したコンテンツを、認証クライアント端末501に送信する。

【0091】（方法例3）前記装置例に適用する本実施形態例の方法例3につき図6及び図10を参照して説明する。方法例3は、あるユーザが第1認証サーバ601において認証をした後、第1認証サーバ601とは異なるサーバである第2認証サーバ701に対して認証をする場合に、適用される手法である。

【0092】そして、方法例3では、第1認証サーバ601（認証トークン発行元）の認証レベルが、第2認証サーバ701（認証トークン利用先）の認証レベルよりも低いと、仮定する。先ず、前述の方法例1と同様に、ユーザが認証サーバ群（第1認証サーバ601及び第2認証サーバ701）に対して、初めて認証を行うとする。その後、第1認証サーバ601とは異なる第2認証サーバ701に対して、認証要求を行うとする。このときの処理手順が図10に示されている。

【0093】図10は、認証トークン発行先の認証サーバの認証レベルが認証トークン利用先の認証サーバの認証レベルよりも低い場合の処理手順を示すフローチャートである。

【0094】先ず、ユーザは、認証クライアント端末501の処理プログラム502を起動させて、その処理プログラム502に含まれているコンテンツ要求部503から第2認証サーバ701の処理プログラム702の認証開始部708に対して、第1認証サーバ601で作成された認証トークンを伴ったコンテンツ要求情報を送信することで、コンテンツを要求する。

【0095】認証開始部708は、コンテンツ要求情報を受けた後、その要求内容が認証を必要とするものか判断し、認証が必要である場合は認証処理部709を呼び出す。認証処理部709は、コンテンツ要求情報に「認証済みの認証トークン」が付属していることを確認し、「信頼するサーバリスト707」を参照して、信頼するサーバによって作成された認証トークンであることを確認する。

【0096】次いで、問合せ電文作成部727は、図6(b)に示す問合せ電文を作成し、認証トークン発行元の第1認証サーバ601の処理プログラム602の問合せ電文受付部629に暗号化された電文を送信する。

【0097】問合せ電文受付部629は、第1認証サーバ601と第2認証サーバ701の認証レベルを比較し、第1認証サーバ601の認証レベルが第2認証サーバ701の認証レベルよりも低いと判断した場合は、認証トークン検査/更新部616において、第1認証サーバ601に保管されていた認証トークンを削除し、回答電文作成部630において図6(d)に示す回答電文を作成し、第2認証サーバ701の回答電文受付部728に送信する。

【0098】図6(d)は、回答電文作成部630で作成された回答電文の構造を示す概念模式図である。その後、回答電文受付部728は、受け取ったクライアント

情報と有効期限を認証トークン作成部 711 に渡す。

【0099】認証トークン作成部 711 は、新たに認証トークンを作成し、その認証トークンをコンテンツ返却部 710 に渡す。コンテンツ返却部 710 は、「信頼されるサーバリスト」707 に基づき、第 2 認証サーバ 701 で新たに作成された認証トークンを添付して、WWWコンテンツ 703 から取得したコンテンツを、認証クライアント端末 501 に送信する。

【0100】

【実施例】最後に、以上の装置例及び方法例で説明したシングルサインオン認証システムを用いて、利用者課金をするビジネスモデルにつき実施例として説明する。図 11 は、本発明の一実施例に係る利用者認証システム装置の構成図である。同図において、端末装置 1, 1, 1, … が図 1 に示す認証クライアント端末 501 に該当し、認証サーバ 12 が図 1 に示す第 1 認証サーバ 601 及び第 2 認証サーバ 701 に該当する。

【0101】この一実施例に係る利用者認証システム装置 8 は、ネットワーク 2 上に、複数の業務サーバ 3, 3, 3, … (業務サーバ群 10) との間のネットワーク接続を可能とするよう設定された代理認証機構 5 と、複数の業務サーバ 3, 3, 3, … を利用する全ての端末装置 1, 1, 1, … (端末装置群 11) の利用者認証を可能とするよう設定されたパスワードデータベース 4 及び課金データベース 9 とからなる認証サーバ 12 を有して構成される。

【0102】ここで、認証サーバ 12 における代理認証機構 5 には、当該認証サーバ 12 の手続業務により、全ての端末装置 1, 1, 1, … の各利用者から業務サーバ利用料の集計額を複数の業務サーバ 3, 3, 3, … に代わって代理徴収すると共に、当該複数の業務サーバ 3, 3, 3, … から業務サーバ利用料の徴収代行手数料として認証サーバ使用料を徴収するために、パスワードデータベース 4 及び課金データベース 9 を参照することにより、全ての端末装置 1, 1, 1, … の各利用者についての業務サーバ利用料を定期的に集計する処理過程を実行するための処理手段 (図示せず) が新たに具備される。

【0103】以上の構成において、端末装置群 11 における特定の端末装置 1 が、業務サーバ群 10 に含まれる何れかの業務サーバ 3 を用いてある業務を行った場合、認証サーバ 12 は、パスワードデータベース 4 及び課金データベース 9 のデータに基づき、端末装置 1 の利用者から業務サーバ利用料の代理徴収を行うと共に、その代理徴収に係る業務サーバ利用料を個々の業務サーバ 3, 3, 3, … へ定期的に支払い、さらに、個々の業務サーバ 3, 3, 3, … から徴収代行手数料としての認証サーバ使用料を定期的に徴収する (支払いを受ける)。

【0104】そして以上により、本来は個々の業務サーバ 3, 3, 3, … にて実施すべき利用者課金業務を、上

記認証サーバ使用料を運営資金としながら認証サーバ 12 において一括して代行することが可能となり、これに伴い、個々の業務サーバ 3, 3, 3, … にて個別に利用者課金業務を行う必要がなくなると、それら個々の業務サーバ 3, 3, 3, … の運営管理コストの削減を図ることが可能となる。

【0105】以上、本発明の実施形態を説明したが、本発明は、必ずしも上記した事項に限定されるものではなく、本発明の目的を達し、下記する効果を奏する範囲において、適宜変更実施可能である。例えば、第 1 認証サーバ 601 及び第 2 認証サーバ 701 としては、パーソナル・コンピュータに限らず、PDA (Personal Digital Assistants)、携帯電話、パーソナル・ハンディホン・システム (PHS)、カーナビゲーションシステム、ゲーム機器等を用いることが可能である。

【0106】また、ネットワーク 2 としては、インターネット及びイントラネットに限らず、エキストラネット、ローカル・エリア・ネットワーク (LAN)、公衆電話回線、専用電話回線などを用いたものでもよい。

【0107】

【発明の効果】以上説明したように、本発明によれば、ユーザが 1 回のログインで、複数のサーバにアクセスできるようにするシングルサインオンを提供するシステムにおいて、ユーザの認証状態を複数のサーバで共有する際に、各サーバがユーザの認証状態を分散管理することを可能とするので、認証状態を一元管理する認証状態管理サーバを必要とせずにシングルサインオン・システムを構築することが可能となり、システム構築コスト及び運用管理コストを軽減することが可能となる。

【0108】また、複数の認証サーバ間において認証に関する信頼性につき優劣がある場合に、その信頼性の優劣に応じて各サーバでユーザの認証状態を分散管理するので、複数の認証に関する情報から信頼性の高い情報を選択して認証することが可能となり、認証についての信頼性を高めると共に、信頼関係の変化に柔軟に対応した認証状態の共有をすることが可能となる。

【0109】また、各サーバ間で共同利用される認証状態を示す情報 (認証トークン) につき、サーバの署名の添付及び暗号化を施してネットワーク上を伝送することで、認証についての高度なセキュリティを確保することが可能となる。

【図面の簡単な説明】

【図 1】本発明の実施形態である装置例の概念模式図である。

【図 2】同上の装置例の動作を示すフローチャートである。

【図 3】同上の装置例におけるデータベースの構造を示す図であり、(a) は認証データベースの構造を示し、(b) は認証状態管理データベースの構造を示している。

【図 4】本発明の実施形態である方法例 1 において、ユーザが認証サーバ群に初めて認証を求めるときの手順を示すフローチャートである。

【図 5】同上の方法例 1 における認証トークン作成部 611 での処理手順を示すフローチャートである。

【図 6】同上の装置例で作成される各種電文の構造を示す概念模式図であり、(a) は認証トークンの構造であり、(b) は問合せ電文の構造であり、(c) は回答電文の構造であり、(d) は他の回答電文の構造である。

【図 7】同上の方法例 1 における同一の認証サーバに再度の認証要求が発生した場合の処理手順を示すフローチャートである。

【図 8】同上の方法例 1 における認証トークン検証／更新部 616 の処理手順を示すフローチャートである。

【図 9】本発明の実施形態である方法例 2 において、認証トークン発行元の方が認証トークン利用先よりも認証レベルが高い場合の処理手順を示すフローチャートである。

【図 10】本発明の実施形態である方法例 3 において、認証トークン発行元よりも認証トークン利用先の方が認証レベルが高い場合の処理手順を示すフローチャートである。

【図 11】本発明の一実施例に係る利用者認証システム装置の構成図である。

【図 12】従来のシングルサインオン機能を持ったシステム装置の模式概念図である。

【図 13】同上のシステム装置の処理手順を示すフローチャートである。

【符号の説明】

δ ……一実施例に係る利用者認証システム装置

1 ……端末装置

2 ……ネットワーク

3 ……業務サーバ

4 ……パスワードデータベース

5 ……代理認証機構

9 ……課金データベース

10 ……業務サーバ群

11 ……端末装置群

12 ……認証サーバ

101, 501 ……認証クライアント端末

102, 202, 302, 402, 502, 602, 702 ……処理プログラム

201, 301, 601, 701 ……認証サーバ

203, 303, 603, 703 ……WWWコンテンツ

403, 604, 704 ……認証データベース

404, 605, 705 ……認証状態管理データベース

606, 706 ……信頼されるサーバリスト

607, 707 ……信頼するサーバリスト

503 ……コンテンツ要求部

504 ……認証処理部

608 ……認証開始部

609 ……認証処理部

610 ……コンテンツ返却部

611 ……認証トークン作成部

612 ……有効期限作成部

613 ……認証 ID 作成部

614 ……署名作成部

615 ……共通鍵暗号部

616 ……認証トークン検証／更新部

617 ……認証トークン発行者検証部

618 ……共通鍵復号部

619 ……署名検証部

620 ……認証 ID 検証部

621 ……クライアント情報検証部

622 ……有効期限検証部

623 ……有効期限更新部

624 ……認証 ID 更新部

625 ……署名作成部

626 ……共通鍵暗号部

629 ……問合せ電文受付部

630 ……回答電文作成部

708 ……認証開始部

709 ……認証処理部

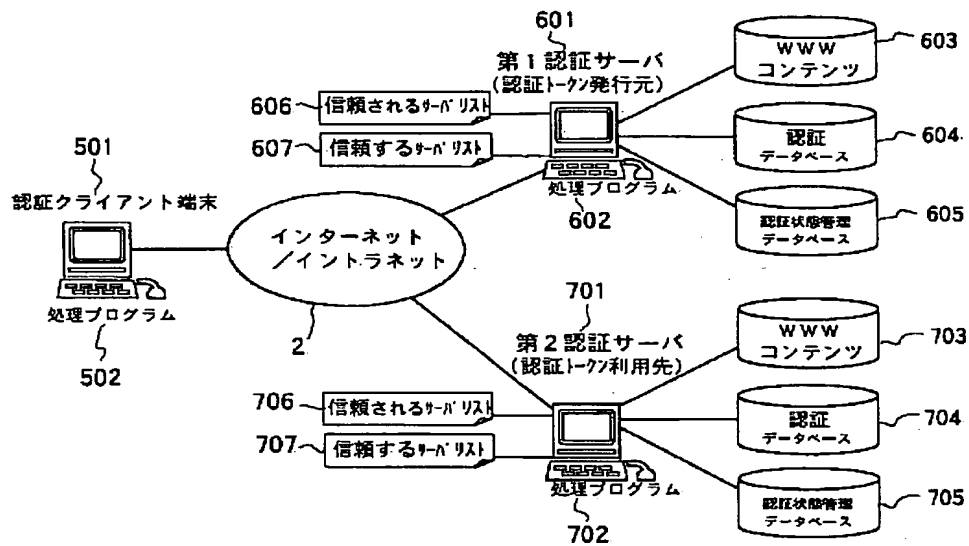
710 ……コンテンツ返却部

711 ……認証トークン作成部

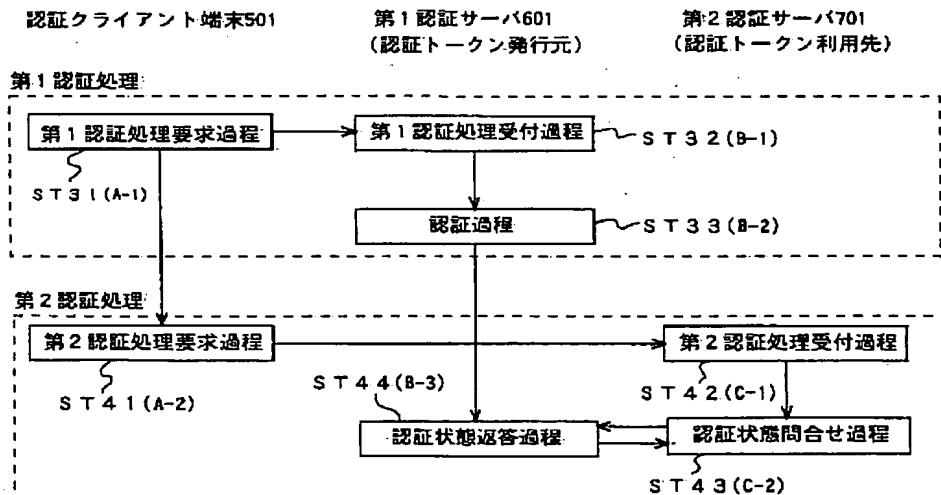
727 ……問合せ電文作成部

728 ……回答電文受付部

【図 1】



【図 2】



【図 3】

認証データベース

カラム名	説明
ユーザID	認証対象のユーザID
パスワード	認証対象のユーザのパスワード
⋮	その他、ユーザを特定する情報

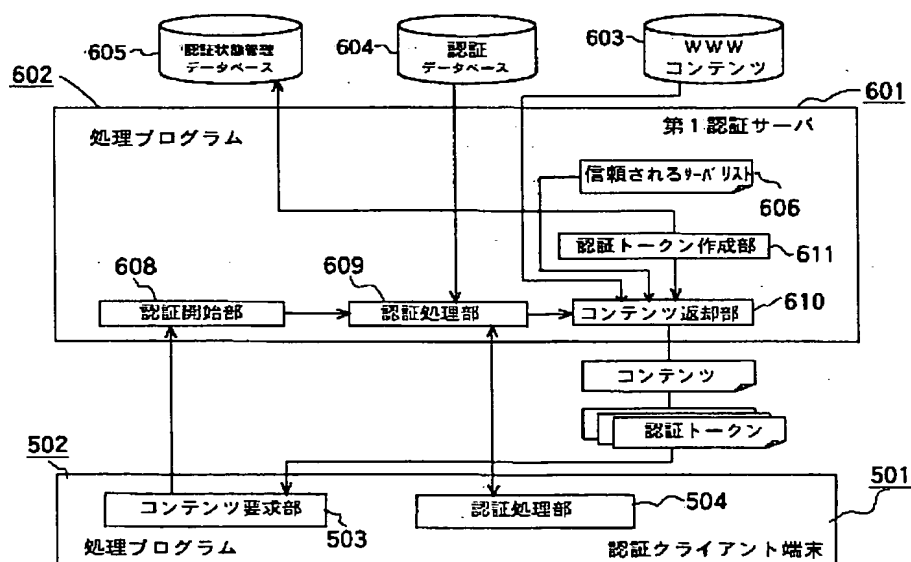
(a)

認証状態管理データベース

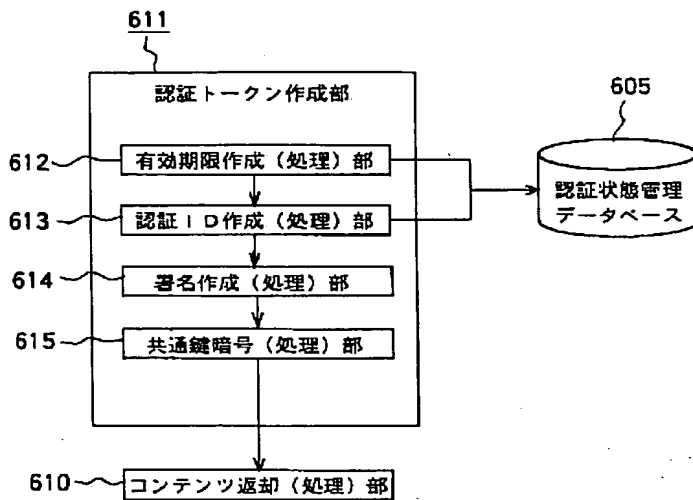
カラム名	説明
ユーザID	認証済みユーザID
認証ID	アクセスごとに変更する一時的なID
クライアントアドレス	クライアントアドレス
有効期限	認証状態の有効期間
⋮	その他、クライアントを特定する情報

(b)

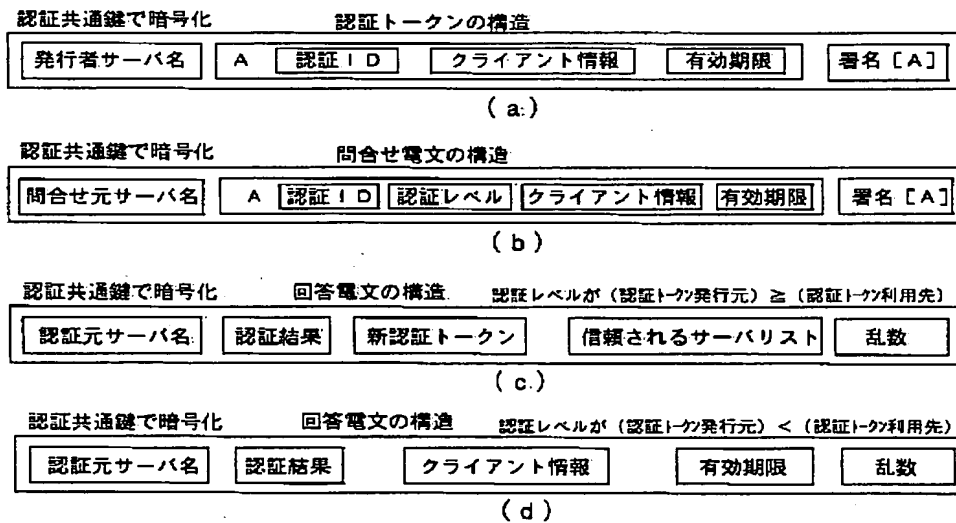
【図 4】



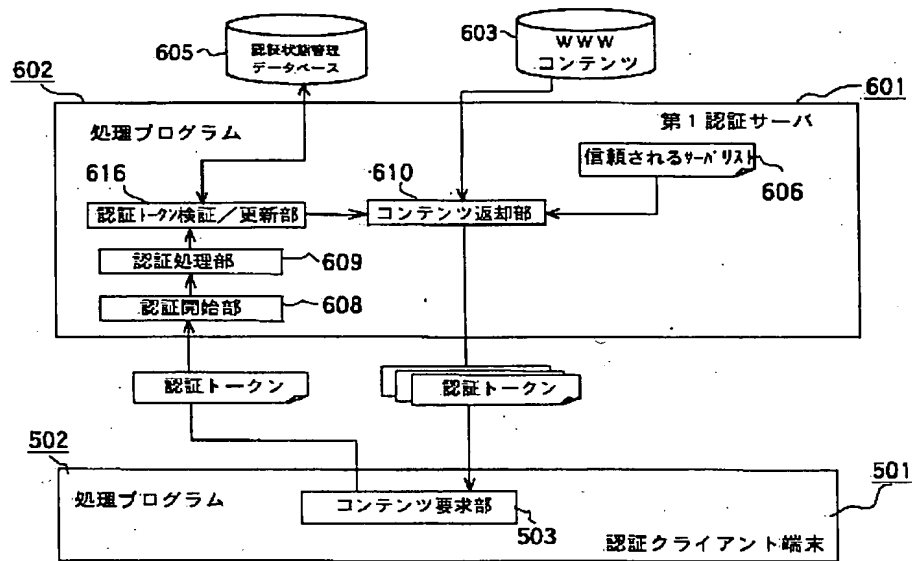
【図 5】



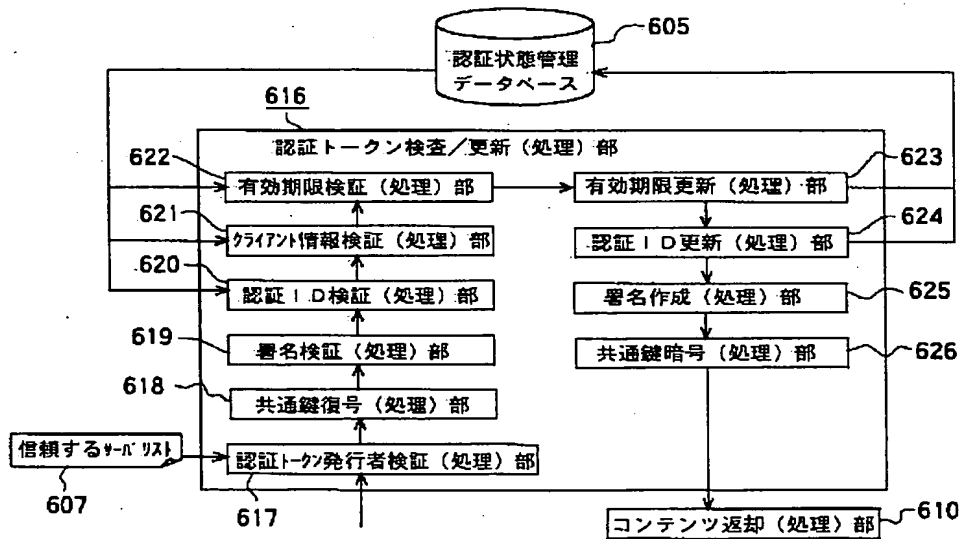
【図 6】



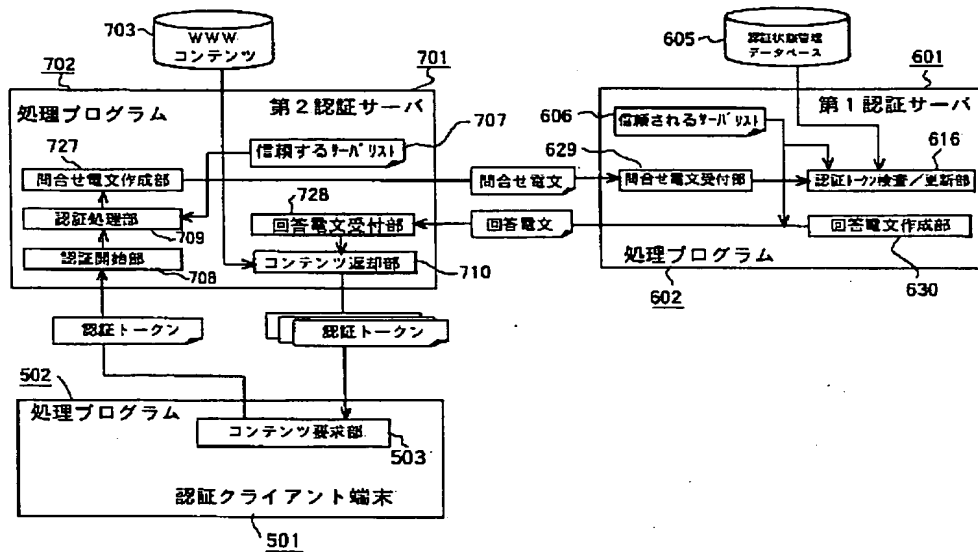
【図 7】



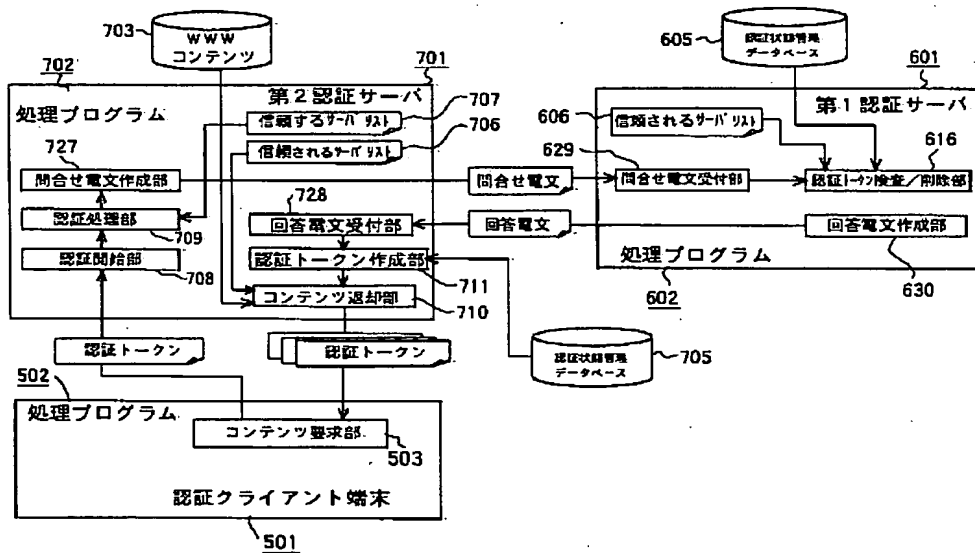
【図 8】



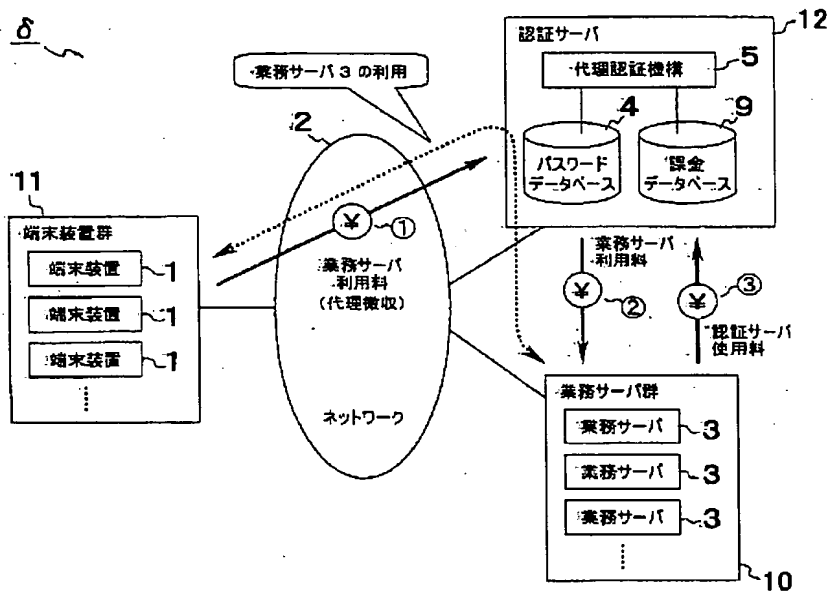
【図 9】



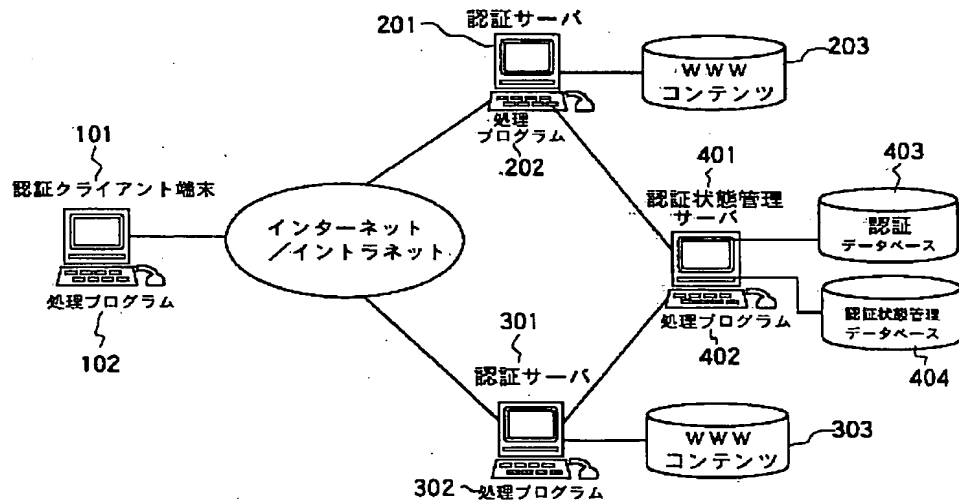
【図 10】



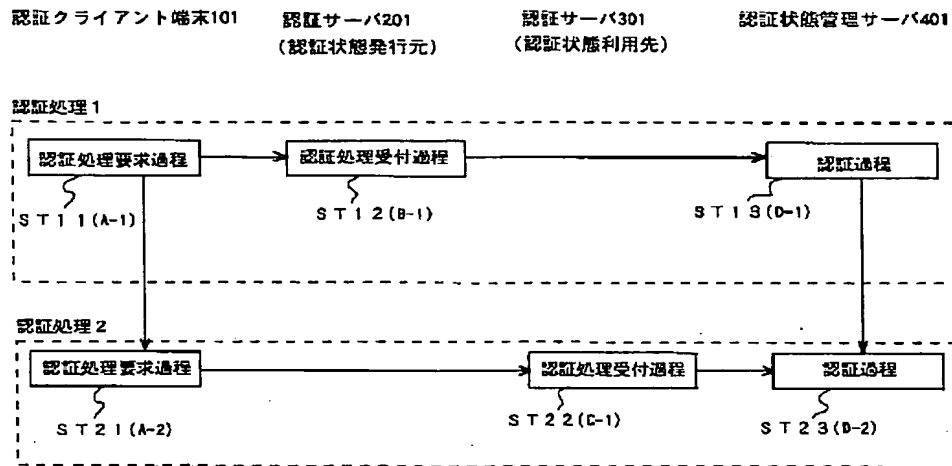
【図 11】



【図 12】



【図 13】



フロントページの続き

Fターム(参考) 5B085 AE00 AE02 BC01
5J104 AA08 KA01 KA02 MA03 NA05
PA07

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.